日　本　国　特　許　庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。
This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２０００年　２月２４日

出願番号
Application Number: 特願２０００－０４７３２３

出願人
Applicant (s): 日本電信電話株式会社

２０００年　６月２３日

特許庁長官
Commissioner,
Patent Office 近藤隆彦

出証番号　出証特２０００－３０４６８３８

【書類名】　特許願

【整理番号】　NTTH116889

【提出日】　平成12年 2月24日

【あて先】　特許庁長官殿

【国際特許分類】　G09C

【発明者】

【住所又は居所】　東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内

【氏名】　小林　邦生

【発明者】

【住所又は居所】　東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内

【氏名】　森田　光

【特許出願人】

【識別番号】　000004226

【氏名又は名称】　日本電信電話株式会社

【代理人】

【識別番号】　100066153

【弁理士】

【氏名又は名称】　草野　卓

【選任した代理人】

【識別番号】　100100642

【弁理士】

【氏名又は名称】　稲垣　稔

【手数料の表示】

【予納台帳番号】　002897

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　　図面　1

【物件名】　　要約書　1

【包括委任状番号】　9806848

【プルーフの要否】　　要

【書類名】　　明細書

【発明の名称】　大小比較方法、その装置及びプログラム記録媒体

【特許請求の範囲】

【請求項１】　参加者ｊはＮ種の指標値１，２，…，Ｎから選んだ意中の指標値i_jと、初期値IV_jと、１以上の任意の整数x_jを参加者装置に入力し、

参加者装置はIV_jに一方向性関数ｇをx_j回施し、その値$g^{xj}(IV_j)$に対し、ｇと異なる一方向性関数ｈをＮ－i_j回施し、その値$A_j=h^{N-ij}(g^{xj}(IV_j))$を中央装置へ送って意中の指標値$i_j$を間接的に登録し、

中央装置は全参加者装置からA_jを受信後に、ｋ＝Ｎ，Ｎ－１，Ｎ－２，…と順次、ｋで登録したかどうかの問合せを各参加者装置へ送信し、

各参加者装置は受信した問合せｋが自分の意中の指標値とは異なる場合は$B_{k,j}=h^{k-ij-1}(g^{xj}(IV_j))$を中央装置へ送信し、

中央装置は受信した$B_{k,j}$に一方向性関数ｈを施し、$h(B_{k,j})=A_j$となることを検証し、A_jの値を受信した$B_{k,j}$に変更し、

自分の意中の指標値と問合せのｋが同一である参加者ｊの装置は$B_{k,j}=g^{xj-1}(IV_j)$を中央装置へ送り、

中央装置は受信した$B_{k,j}$に一方向性関数ｇを施し、$g(B_{k,j})=A_j$となることを検証し、

自分の意中の指標値がｋで上記順次の問合せに対し、初めてある参加者ｊの意中の指標値がｋと同一であることが検証されたとき、その指標値ｋを全参加者の意中値のうちの最大値として出力することを特徴とする大小比較方法。

【請求項２】　請求項１記載の方法において、

自分の意中の指標と問合せのｋが同一である参加者ｊの装置は同一であることを示す同一情報も中央装置へ送り、

中央装置は参加者装置からの受信情報中に同一情報が含まれていない場合は、上記$h(B_{k,j})=A_j$かの検証を行い、同一情報が含まれている場合は上記$g(B_{k,j})=A_j$の検証を行うことを特徴とする大小比較方法。

【請求項３】　請求項１記載の方法において、

中央装置は上記$h(B_{k,j})=A_j$の検証において不一致の場合は上記$g(B_{k,}$

$_j$）＝A_jの検証を行うことを特徴とする大小比較方法。

【請求項４】　請求項１乃至３の何れかに記載の方法において、

上記Ｎ種の指標値１，２，…，ＮはＮ個の値P_1，P_2，…，P_Nとその大小順に対応付けられてあり、

参加者はP_1，P_2，…，P_Nから選んだ意中の１つを参加者装置に入力することにより上記指標値i_jの入力を行い、

上記全参加者の意中指標値のうちの最大値ｋと対応する値P_kを最大値又は最小値として出力することを特徴とする大小比較方法。

【請求項５】　Ｎ種の指標値１，２，…，Ｎから選んだ１つの指標値i_j、初期値IV_j、１以上の任意の整数値x_jを入力する入力手段と、

入力値に対し、一方向性関数ｇを施すｇ演算手段と、

入力値に対し、一方向性関数ｈを施すｈ演算手段と、

記憶手段と、

中央装置と情報の送受信を行う送受信手段と、

指標値i_j、初期値IV_j、整数値x_jを記憶手段に記憶し、$A_j=h^{N-ij}(g^{xj}(IV_j))$を生成して中央装置へ送り、中央装置からｋ登録かの問合せを受信すると、$k\neq i_j$であれば$B_{k,j}=h^{k-ij-1}(g^{xj}(IV_j))$を生成し、$k=i_j$であれば、$B_{k,j}=g^{xj-1}(IV_j)$を生成して$B_{k,j}$を中央装置へ送信する制御手段と、

を具備する参加者装置。

【請求項６】　請求項５記載の装置において、

P_1，P_2，…，P_Nなる値をその大小順に上記指標値１，２，…，Ｎを対応付けた換算テーブルを備え、

上記入力手段に指標値i_jに代え、P_1，P_2，…，P_Nから選んだ１つの値$P_{k,j}$が入力され、

上記制御手段は、入力された値P_jを上記換算テーブルを参照して指標値i_jに変換することを特徴とする参加者装置。

【請求項７】　複数の参加者装置から間接的に登録された意中の指標値の大小関係を比較する装置であって、

記憶手段と、

入力値に対し、一方向性関数ｇを施すｇ演算手段と、

入力値に対し、一方向性関数ｈを施すｈ演算手段と、

各値ｋから１つずつ減算する減算手段と、

各参加者装置と情報の送受信を行う送受信手段と、

各参加者装置からの登録情報A_jを記憶手段に記憶し、全参加者装置からの登録情報A_jの受信後に、上記値ｋを指標値の最大値Ｎに設定し、各参加者装置に値ｋで登録を行ったかの問合せを送り、その応答情報$B_{k,j}$に対し一方向性関数ｈを施し、その値ｈ（$B_{k,j}$）が対応するA_jと等しいことを確認し、そのA_jの値を受信した$B_{k,j}$の値に変更し、全参加者装置からの応答情報を処理するとｋを－１して問合せをすることを繰返し、登録した意中の指標値と問合せのｋが同一である参加者装置の応答情報$B_{k,j}$に対し、一方向性関数ｇを施し、その値ｇ（$B_{k,j}$）が対応するA_jと等しいことを確認して、そのｋが全登録指標値中の最大値として出力する制御手段と

を具備する中央装置。

【請求項８】　請求項７記載の装置において、

Ｎ種の指標値１，２，…，Ｎに対し、Ｎ個の値P_1，P_2，…，P_Nをその大小順に対応付けた換算テーブルを備え、

制御手段は上記最大値とした指標値ｋと対応する値P_kを換算テーブルを参照して、全登録値中の最大値又は最小値として出力することを特徴とする中央装置。

【請求項９】　参加者装置から、Ｎ種の指標値１，２，…，Ｎから選んだ１つの指標値i_jを中央装置に間接的に登録し、中央装置で全登録指標値中の最大値を求めシステムにおける参加者装置のコンピュータに、

入力された指標値i_j、初期値IV_j、１以上の任意の整数x_jを記憶手段に記憶する処理と、

IV_jに対し一方向性関数ｇをx_j回施して$g^{xj}(IV_j)$を得る処理と、

$g^{xj}(IV_j)$に対し、一方向性関数ｈをＮ－i_j回施して$A_j = h^{N-ij}(g^{xj}(IV_j))$を得る処理と、

A_jを中央装置へ送信する処理と、

中央装置からｋで登録したかの問合せを受信する処理と、

$k = i_j$でなければ$B_{k,j} = h^{k-ij-1}(g^{xj}(IV_j))$を演算する処理と、

$k = i_j$であれば$B_{k,j} = g^{xi-1}(IV_j)$を演算する処理と、

$B_{k,j}$を中央装置へ送信する処理と

を実行させるプログラムを記録した記録媒体。

【請求項１０】　請求項９記載の記録媒体において、

入力された値P_jを、指標値１，２，…，Ｎに対し、値P_1，P_2，…，P_Nが大小順に対応付けられた換算テーブルを参照してi_jに変換して、i_jを入力する処理を

上記コンピュータに実行させるプログラムを上記プログラムが含むことを特徴とする記録媒体。

【請求項１１】　複数の参加者装置から、Ｎ種の指標値１，２，…，Ｎから選んだ１つの指標値i_jを登録情報A_jによりそれぞれ中央装置に間接的に登録し、中央装置で全登録指標値中の最大値を求める中央装置のコンピュータに、

各参加者装置からの登録情報A_jを受信する処理と、

受信した登録情報A_jを記憶手段に記憶する処理と、

全参加者装置からの登録情報A_jを受信した後に、値ｋにＮを設定してｋで登録したかの問合せを各参加者装置へ送信する処理と、

問合せに対する応答情報$B_{k,j}$を受信する処理と、

ｋに対する登録をしてない参加者装置からの$B_{k,j}$に対し一方向性関数ｈを施しｈ（$B_{k,j}$）を求める処理と、

受信$B_{k,j}$と対するA_jを記憶手段から読出して、ｈ（$B_{k,j}$）＝A_jであるかを検証する処理と、

ｈ（$B_{k,j}$）＝A_jであれば、A_jとして$B_{k,j}$を記憶手段に記憶する処理と、

全参加者装置から応答情報を受信すると、ｋを１減算して上記問合せ処理以下を繰返す処理と、

ｋに対する登録をしている参加者装置からの$B_{k,j}$に対し、一方向性関数ｇを施してｇ（$B_{k,j}$）を求める処理と、

$B_{k,j}$と対応するA_jを記憶手段から読出して$g(B_{k,j})=A_j$であるかを検証する処理と、

その検証に合格すると、そのｋを全登録指標値の最大値として出力する処理とを実行させるプログラムを記録した記録媒体。

【請求項１２】　請求項１１記載の記録媒体において、

上記最大値としたｋにより、指標値１，２，…，Ｎに対し、値P_1，P_2，…，P_Nが大小順に対応付けられた換算テーブルを参照して値P_kを最大値又は最小値として出力する処理を上記コンピュータに実行させるプログラムを上記プログラムが含むことを特徴とする記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

この発明は情報セキュリティ技術の応用技術に関するものであり、特にインターネットなどにより多数の参加者がオンラインでアクセス可能な状況下で、各々の秘密値の大小を比較する方法に関するものであり、電子くじ、電子投票、電子入札など様々なアプリケーション（応用分野）での利用が可能である。

【０００２】

【従来の技術】

例えば電子競争入札は図７に示す様に、参加者毎に設けられる参加者装置、この場合は入札装置11_1，11_2，…，11_Mと、これらと例えばネットワークで接続され、全体を統合的に処理する中央装置、この場合は開票装置１２から構成され、各１，２，３，…，ＮのＮ種の指標値に対応して、初期値ＩＶに一方向性関数ｈを多重に施し、つまりＩＶにｉ回の一方向性関数を施す場合、$h^i(IV)$と表現し、これはｈ（ｈ（ｈ（…ｈ（ＩＶ）…））（このｈの数はｉ）を意味する。これらｈ（ＩＶ），$h^2(IV)$，$h^3(IV)$，…，$h^N(IV)$なる値をそれぞれ指標値１，２，３，…，Ｎと対応させることとし、各参加者ｊ（ｊ＝１，２，…，Ｍ）はその入札装置11_jから$A_j=(h^{N+1}(IV_j), g(h^{ij}(IV_j)))$なる一対の値を生成して、開票装置１２に送ることで、その参加者ｊの意中の指標値（秘密値）i_jを間接的に登録する。ｇ（Ａ）はＡに一方向

性関数ｇを施すことを表わし、またその明細書ではi_jを添字として用いる場合は例えば「^{ij}」と表記する。開票装置１２は全参加者からの登録を受信した後、カウンタ１３を初期値Ｎから順次ダウンカウントし、そのカウンタ１３の各値ｋ（Ｎ，Ｎ－１，…，１）について登録した参加者ｊがいるかどうかを、全参加者端末装置11_1，…，11_Mに順次ｋを送信して尋ね、各入札装置11_jは該当しないときは、$B_{k,j}=h^k(IV_j)$を開票装置１２へ応答し、開票装置１２は$h(B_{k,j})=A_j$および$g(B_{k,j})\neq C_j$となることを確認して、その参加者ｊの意中の指標値がｋではないということを証明し、A_jの値を受信した$B_{k,j}$に変更して次のｋに備え、

問合せに対し自分の意中の指標値とｋが同一である参加者ｊは$B_{k,j}=h^k(IV_j)$を開票装置１２へ送り、開票装置１２は受信した$B_{k,j}$に対し、$h(B_{k,j})=A_j$および$g(B_{k,j})=C_j$となることを確認して、その参加者ｊの意中の指標値がｋであることを証明する。

【０００３】

初めてある参加者の意中の指標値がｋであるものが現われ、かつこれが証明されたとき、そのｋを登録した全指標値中の最大値であることとする。

【０００４】

【発明が解決しようとする課題】

従来の方法ではその値の正当性を検証するために、１指標値、１参加者ごとに

$h(B_{k,j})=A_j$

$g(B_{k,j})=C_j$

と２つの式が成立するかの検証が必要であり、指標値数と参加者数の増大により、その処理量が膨大なものとなる欠点があった。

【０００５】

【課題を解決するための手段】

この発明によれば一方向性関数を利用して、秘密値を$h^{N-ij}(g^{xj}(IV_j))$に変換して登録する。x_jは参加者が決める１以上の任意の整数である。また参加者はｋで登録したかの問合せに対し、意中の秘密値でなければ$B_{k,j}=h^{k-ij-1}(g^{xj}(IV_j))$を提示し、意中の秘密値であれば$B_{k,j}=g^{xi-1}(IV_j)$

を提示し、中央装置は前者に対してはｈ（$B_{k,j}$）＝A_jにより、後者に対しては ｇ（$B_{k,j}$）＝A_j により検証する。

【０００６】

【発明の実施の形態】

図１にこの発明の実施例を示す。複数の参加者ｊ（１，２，…，Ｍ）の装置（図には１つのみを示してあるが複数設けられている）１１$_j$ は中央装置１２へ指標値ｉ$_j$を間接的に登録し、中央装置１２でその登録された指標値ｉ$_j$中の最大値を求める。参加者装置１１$_j$は例えば入札装置、中央装置１２は例えば開票装置である。Ｎ種の指標値１，２，…，Ｎに対し、Ｎ個の値P_1，P_2，…，P_Nが大小順に対応付けられた換算テーブル２１が各入札装置１１$_j$ と開票装置１２に設けられる。図１の例はP_1＝１０，P_2＝１５，P_3＝３０，…，P_N＝３０００と指標値ｋ（１，２，…，Ｎ）が大きくなるに従って値P_k が大きくなるように対応付けた場合である。

【０００７】

図２に入札装置１１$_j$ の機能構成を示し、図３にその処理手順を示す。参加者ｊは入力手段２２により、Ｎ個の値P_1，P_2，…，P_Nから１つ選んだ値P_jと、初期値（正整数）ＩＶ$_j$と、１以上の任意の整数ｘ$_j$を入力する（Ｓ１）。制御部２３はＩＶ$_j$，ｘ$_j$を記憶部２４に記憶する（Ｓ２）と共にP_jにより換算テーブル２１を参照してP_jを指標値ｉ$_j$に変換して記憶部２４に記憶する（Ｓ３）。

次にＩＶ$_j$とｘ$_j$を取出してｇ演算部２５に入力して、ＩＶ$_j$に対し、一方向性関数ｇをｘ$_j$回施してg^{xj}（ＩＶ$_j$）を求め（Ｓ４）、必要に応じてこれを記憶部２４に記憶する（Ｓ５）。次にこのg^{xj}（ＩＶ$_j$）、Ｎ、ｉ$_j$をｈ演算部２６に入力して、g^{xj}（ＩＶ$_j$）に対し、一方向性関数ｈをＮ－ｉ$_j$回施して、

$$A_j = h^{N-ij}(g^{xj}(IV_j))$$

を求め（Ｓ６）、送受信部２７へ登録情報としてA_j を開票装置１２へ送信する（Ｓ７）。このようにして参加者ｊは意中の指標値ｉ$_j$ を開票装置１２に間接的に登録する。

【０００８】

開票装置１２の機能構成を図５に、処理手順を図６にそれぞれ示す。開票装置

１２は送受信部３１に各参加者装置１１$_j$からの登録情報Ａ$_j$が受信されると、制御部３２はそのＡ$_j$を記憶部３３に記憶する（Ｓ１）。全参加者装置１１$_j$からの登録情報Ａ$_j$が受信されると（Ｓ２）、カウンタ１３に初期値Ｎを設定し（Ｓ３）、カウンタ１３の計数値ｋで登録したかの問合せを送受信部３１を通じて各参加者装置１１$_j$に送信する（Ｓ４）。

【０００９】

各参加者装置１１$_j$は図３に示すように開票装置１２からの問合せを送受信部２７で受信すると（Ｓ８）、その問合せ指標値ｋが記憶部２４内のｉ$_j$と等しいかを調べ（Ｓ９）、等しくなければつまりｋがその参加者の意中の指標値ｉ$_j$でなければ、記憶部２４からg^{xj}（ＩＶ$_j$）を取り出し、これとｉ$_j$，ｋをｈ演算部２６に入力してg^{xj}（ＩＶ$_j$）に対し一方向性関数ｈをｋ－ｉ$_j$回施して応答情報Ｂ$_{k,j}$を求める（Ｓ１０）。

【００１０】

$$B_{k,j}=h^{k-ij-1}(g^{xj}(IV_j))$$

その応答情報Ｂ$_{k,j}$を送受信部２７から開票装置１２へ送信し、次のｋの問合せを待つ（Ｓ１１）。

開票装置１２は図５に示すように送受信部３１に応答情報Ｂ$_{k,j}$が受信されると（Ｓ５）、Ｂ$_{k,j}$をｈ演算部３４に入力してＢ$_{k,j}$に対し一方向性関数ｈを施す（Ｓ６）。この演算結果ｈ（Ｂ$_{k,j}$）と記憶部３３内のｊに対する登録情報Ａ$_j$と等しいかを調べ（Ｓ７）、ｈ（Ｂ$_{k,j}$）＝Ａ$_j$であればその受信したＢ$_{k,j}$をＡ$_j$として記憶部３３に記憶してＡ$_j$を更新する（Ｓ８）。全参加者装置からの応答情報に対して、同様の処理を行い、全参加者装置からの応答情報に対する処理が終れば（Ｓ９）、カウンタ１３の値ｋを１減算して（Ｓ１０）、そのｋについて登録したかの問合せを各参加者装置に対して行う。

【００１１】

参加者装置１１$_j$において、ｋの問合せが、自分の意中のものであれば、つまり記憶部２４内のｉ$_j$と等しければ（Ｓ９）、図３に示すようにＩＶ$_j$とｘ$_j$－１をｇ演算部２５に入力してＩＶ$_j$に対し一方向性関数ｇをｘ$_j$－１回施して応答情報Ｂ$_{k,j}$＝g^{xj-1}（ＩＶ$_j$）を求め（Ｓ１２）、そのＢ$_{k,j}$を開票装置１２へ送信

する（Ｓ１３）。

応答情報$B_{k,j}$が意中の指標値と等しいことを示すg^{xj-1}（IV_j）の場合は、開票装置１２におけるステップＳ７（図５）でｈ（$B_{k,j}$）が$A_j = h^{ij+1-ij-1}$（g^{xj}（IV_j））＝g^{xj}（IV_j）と等しくならない。そこで$B_{k,j}$をｇ演算部３５に入力して、$B_{k,j}$に対し一方向性関数ｇを施し、ｇ（$B_{k,j}$）を求め（Ｓ１１）、ｇ（$B_{k,j}$）と記憶部３３内のｊに対するA_jと等しいかを調べる（Ｓ１２）。参加者装置11_jが正しい処理をしていたならば、前回のｋ＝i_j＋１に対する問合せ時に、ステップＳ８の処理により$h^{ij+1-ij-1}$（g^{xj}（IV_j））＝g^{xj}（IV_j）＝A_jとなっているから、ｇ（$B_{k,j}$）＝A_jが成立する。このｋを順次減少させる問合せ処理において、最初にｇ（$B_{k,j}$）＝A_jが成立したｋが全参加者の意中の指標値中で最大の値であり、このｋを換算テーブル２１を参照して値P_kに変換し（Ｓ１３）、その値P_kを登録した値中の最大値として出力し、必要に応じてその参加者ｊも出力する（Ｓ１４）。

【００１２】

参加者装置11_jではｋ登録かの問合せを受けた時に、ｋ＝i_jであれば（図３ステップＳ９）、ステップＳ１３で$B_{k,j}$と共に問合せのあったｋと自己の意中のi_jとが等しいことを示す情報（同一を示す情話）も開票装置１２へ送信するようにしてもよい。この場合は開票装置１２では図５中のステップＳ５で$B_{k,j}$を受信すると、同一を示す情報を受信したかを調べ、同一を示す情報を受信していなければｈ（$B_{k,j}$）の演算を行い、同一を示す情報を受信していればｇ（$B_{k,j}$）の演算を行う。なお図５中のステップＳ１２でｇ（$B_{k,j}$）＝A_jとならなければ不正があったとして処理を中止して全員に再登録をさせるとか、あるいはその参加者装置に対する問合せを中止し、他の参加者装置に対する問合せを継続させるようにするなどが考えられる。

【００１３】

また換算テーブル２１として図６に示すように、Ｎ種の指標値１，２，３，…，Ｎに対し、値P_kをその大きい値に３０００，２９１３，２９００，…，１００のように対応付けたものを用いれば、ｋの問合せで最初にｇ（$B_{k,j}$）＝A_jとなったｋと対応するP_kは全参加者の意中の値中の最小値を求めたことになる。

場合によっては換算テーブル２１を使用することなく、指標値の最大値を求めるようにしてもよい。この場合は参加者装置で指標値i_jを入力し、図５中のステップＳ１２の次に、指標値ｋを最大値として出力し、必要に応じてその参加者ｊも出力する。

【００１４】

参加者装置11_j、中央装置１２はそれぞれ、コンピュータにより機能させることもできる。

【００１５】

【発明の効果】

従来の方法ではその値の正当性を検証するために、１指標値、１参加者ごとに

$$h(B_{k,j}) = A_j$$

$$g(B_{k,j}) = C_j$$

が成立するかの２つの検証が必要であったが、この発明ではその値の正当性を検証するために、１指標値、１参加者ごとに

$$h(B_{k,j}) = A_j$$

または

$$g(B_{k,j}) = A_j$$

のいずれか一方が成立するかの検証だけで済み、従来法と比べ、最大値選定または最小値選定を選定されないものの値を明かさないという特徴を保ちつつ処理量を半減できる。

【図面の簡単な説明】

【図１】

この発明の実施例のシステム構成を示す図。

【図２】

図１中の参加者装置11_jの機能構成例を示す図。

【図３】

参加者装置11_jにおける処理手順の例を示す流れ図。

【図４】

図１中の中央装置１２の機能構成例を示す図。

【図５】

中央装置１２における処理手順の例を示す流れ図。

【図６】

換算テーブルの他の例を示す図。

【図７】

従来の電子入札システムを示す図。

【書類名】　図面

【図１】

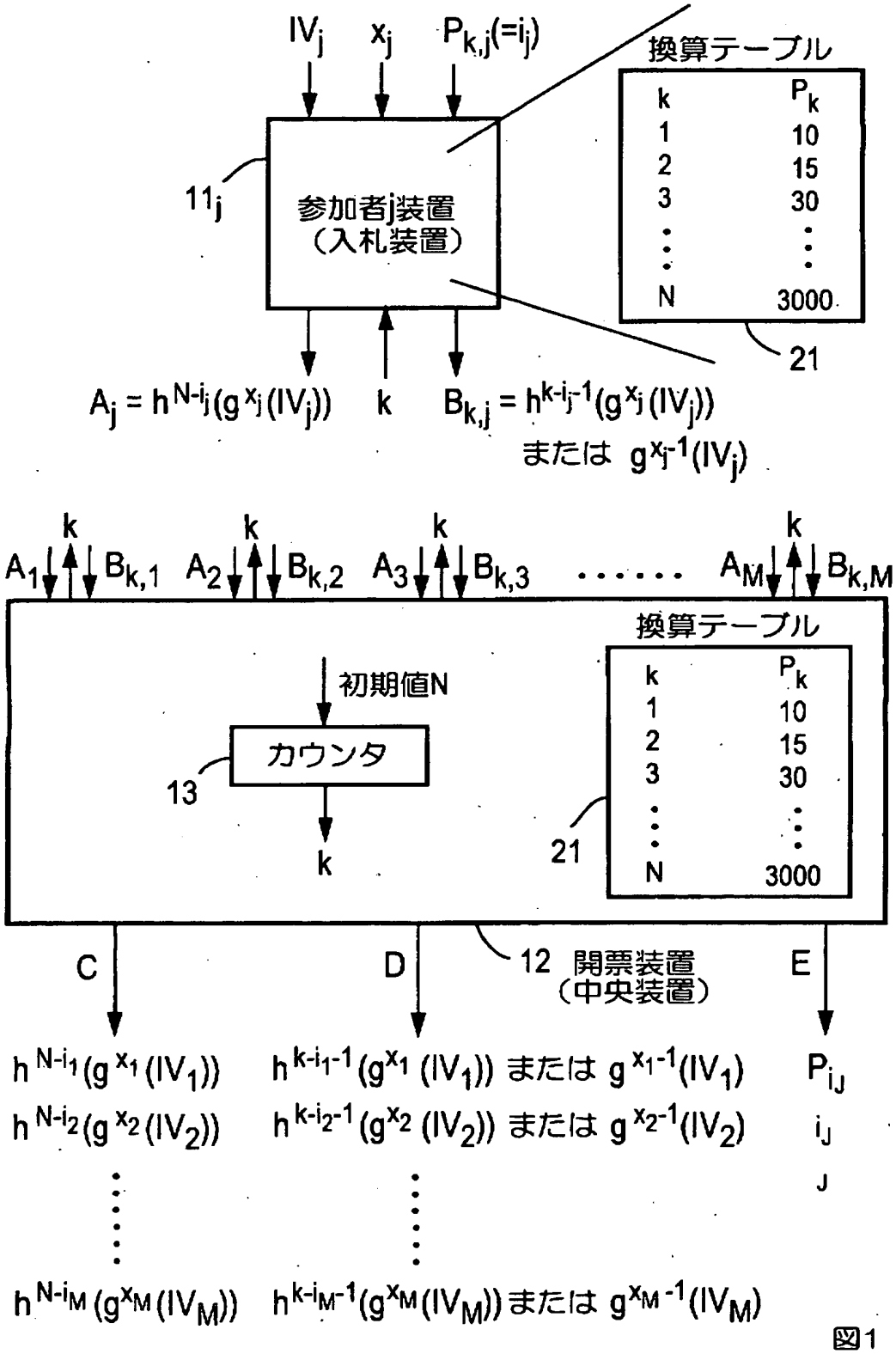
IVj
xj
Pk,j(=ij)
換算テーブル
k
Pk
1
10
2
15
3
30
N
3000
11j
参加者j装置
（入札装置）
21
Aj = h^N-ij(g^xj(IVj))
k
Bk,j = h^k-ij-1(g^xj(IVj))
または g^xj-1(IVj)
A1
Bk,1
A2
Bk,2
A3
Bk,3
AM
Bk,M
初期値N
カウンタ
13
C
D
E
12 開票装置
（中央装置）
h^N-i1(g^x1(IV1))
h^k-i1-1(g^x1(IV1)) または g^x1-1(IV1)
PiJ
h^N-i2(g^x2(IV2))
h^k-i2-1(g^x2(IV2)) または g^x2-1(IV2)
iJ
J
h^N-iM(g^xM(IVM))
h^k-iM-1(g^xM(IVM)) または g^xM-1(IVM)

図1

【図２】

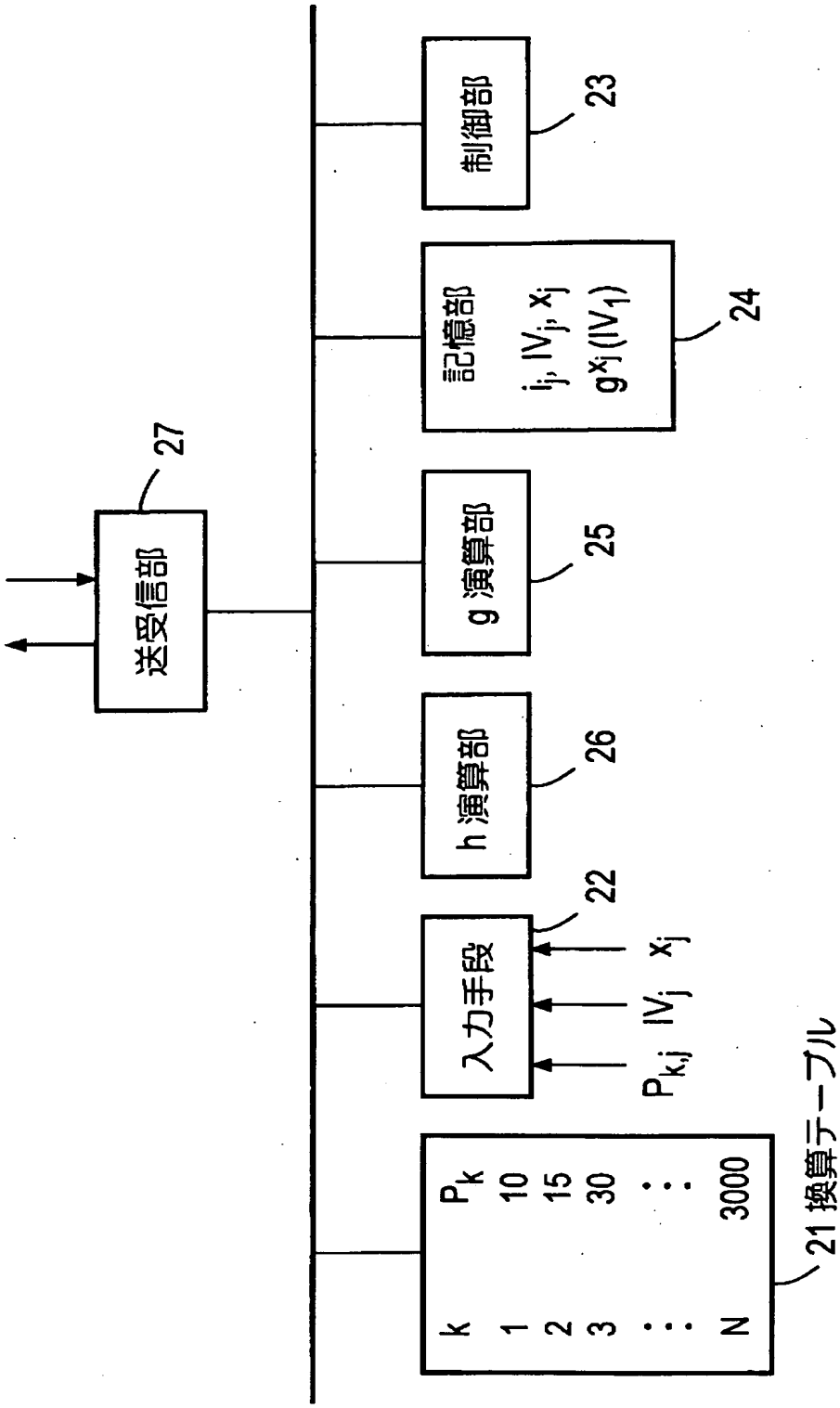
制御部
23
記憶部
i_j, IV_j, x_j
$g^{x_j}(IV_1)$
24
g 演算部
25
h 演算部
26
入力手段
22
$P_{k,j}$ IV_j x_j
送受信部
27
21 換算テーブル
k
1
2
3
N
P_k
10
15
30
3000

図2

【図３】

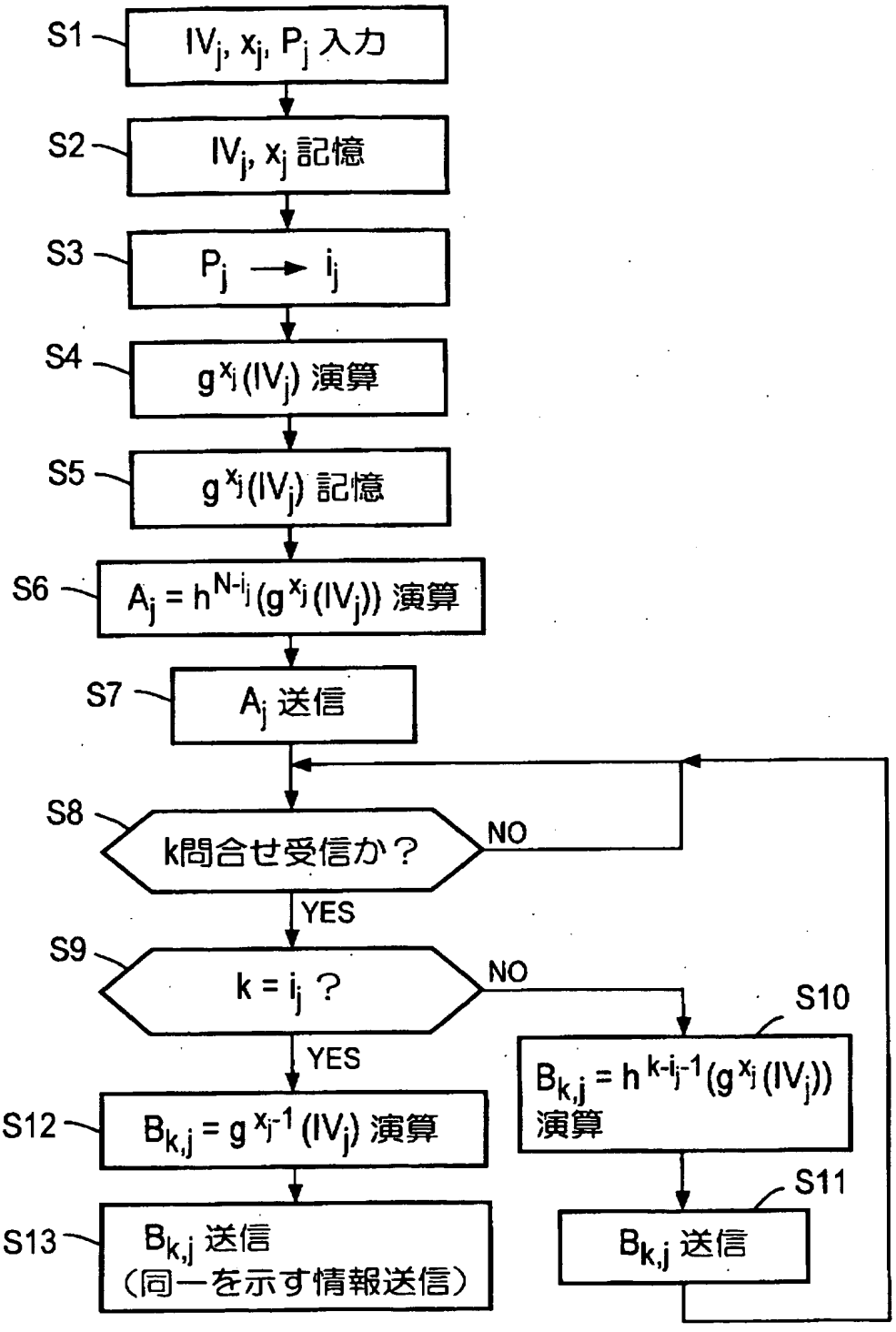
S1
IV_j, x_j, P_j 入力
S2
IV_j, x_j 記憶
S3
$P_j \rightarrow i_j$
S4
$g^{x_j}(IV_j)$ 演算
S5
$g^{x_j}(IV_j)$ 記憶
S6
$A_j = h^{N-i_j}(g^{x_j}(IV_j))$ 演算
S7
A_j 送信
S8
k問合せ受信か？
NO
YES
S9
$k = i_j$ ？
NO
YES
S10
$B_{k,j} = h^{k-i_j-1}(g^{x_j}(IV_j))$ 演算
S11
$B_{k,j}$ 送信
S12
$B_{k,j} = g^{x_j-1}(IV_j)$ 演算
S13
$B_{k,j}$ 送信
（同一を示す情報送信）

図3

【図４】

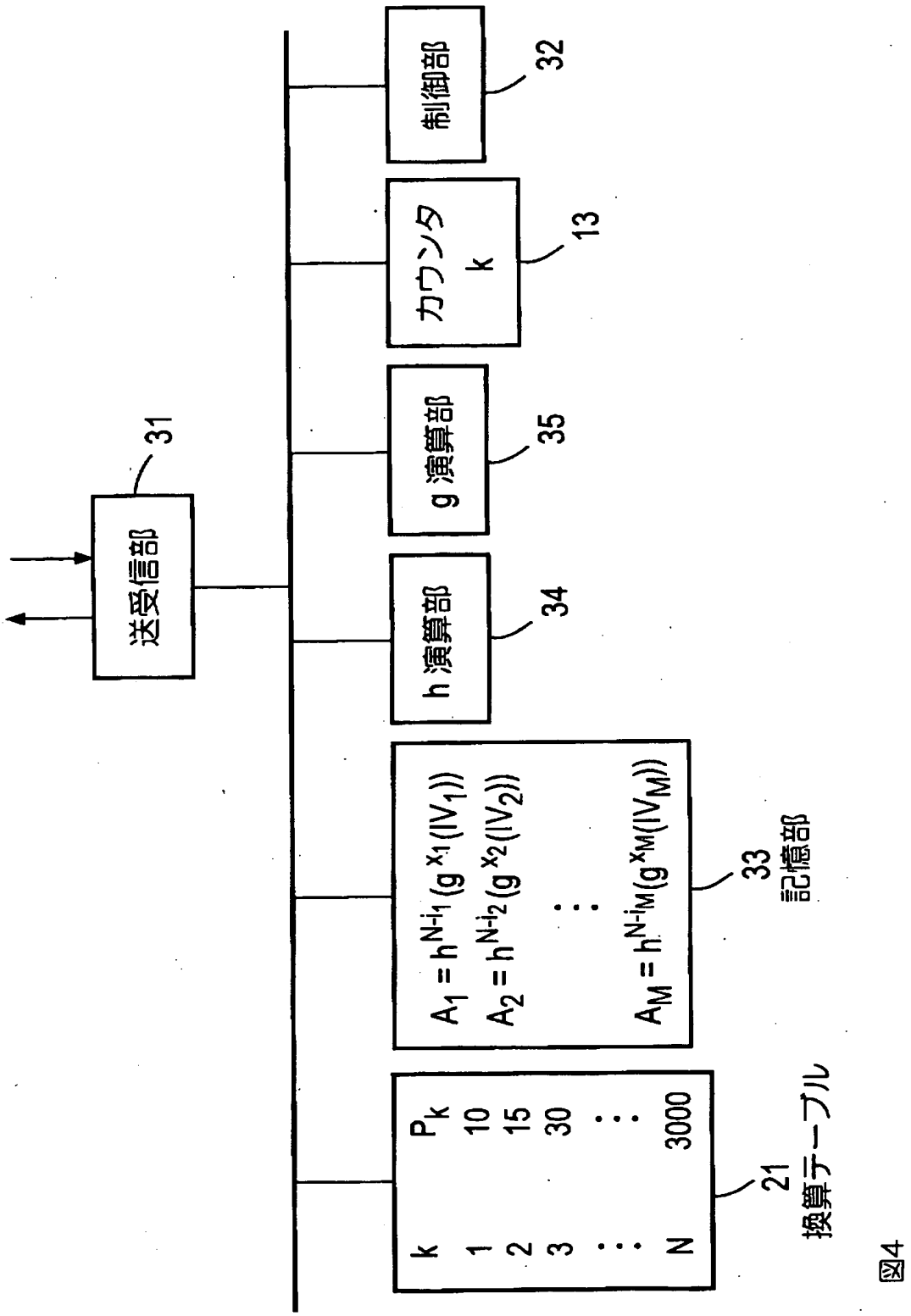
制御部
32
カウンタ
k
13
g 演算部
35
h 演算部
34
送受信部
31
$A_1 = h^{N-i_1}(g^{x_1}(IV_1))$
$A_2 = h^{N-i_2}(g^{x_2}(IV_2))$
$A_M = h^{N-i_M}(g^{x_M}(IV_M))$
33
記憶部
k
1
2
3
N
P_k
10
15
30
3000
21
換算テーブル

図4

【図５】

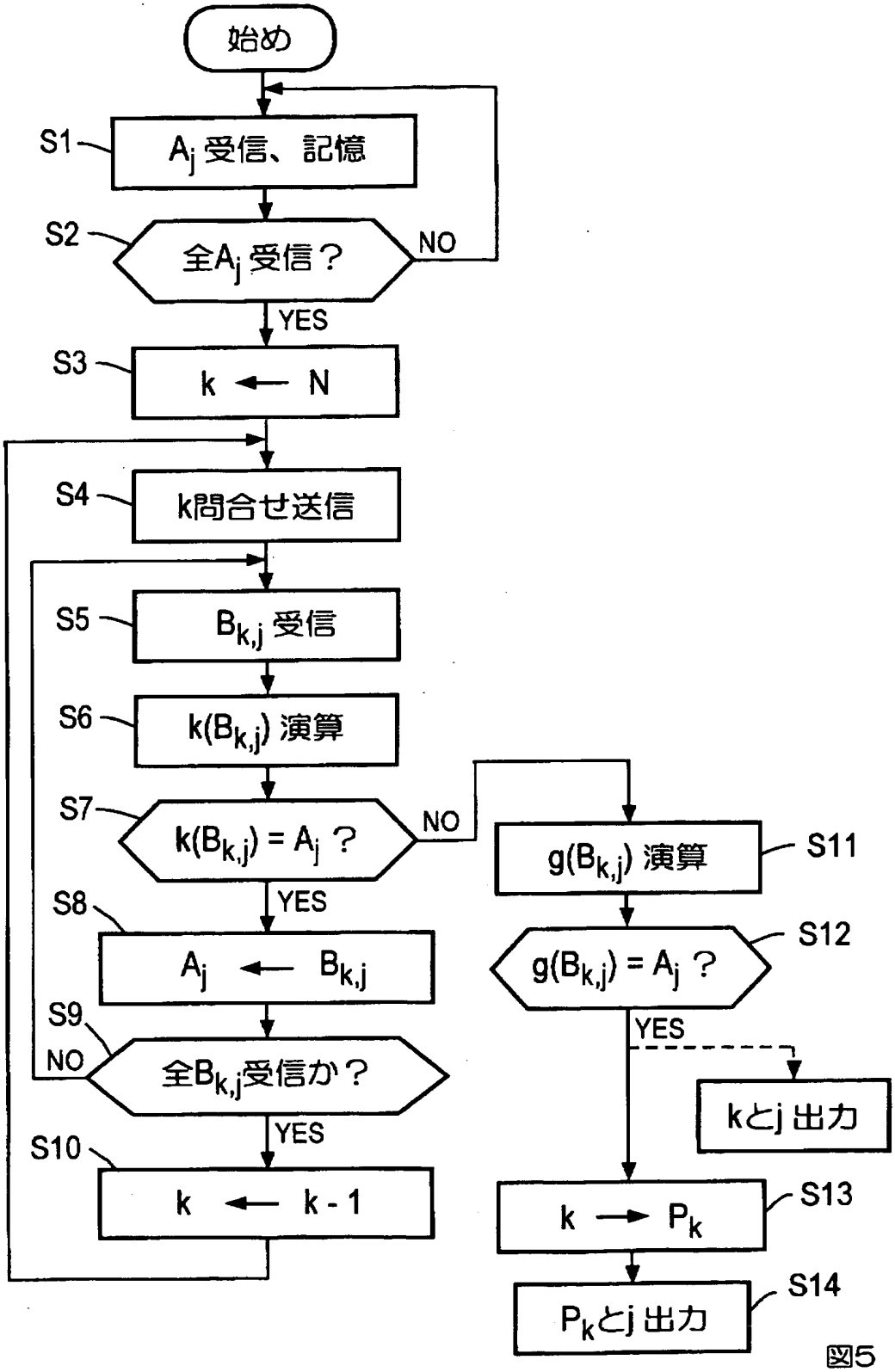
始め
S1
A_j 受信、記憶
S2
全A_j 受信？
NO
YES
S3
k ← N
S4
k問合せ送信
S5
$B_{k,j}$ 受信
S6
$k(B_{k,j})$ 演算
S7
$k(B_{k,j}) = A_j$ ？
NO
YES
S8
A_j ← $B_{k,j}$
S9
NO
全$B_{k,j}$受信か？
YES
S10
k ← k - 1
$g(B_{k,j})$ 演算
S11
$g(B_{k,j}) = A_j$ ？
S12
YES
kとj 出力
k → P_k
S13
P_kとj 出力
S14

図5

【図６】

換算テーブル

k	P_k
1	3000
2	2913
3	2900
⋮	⋮
N	100

21

図6

【図７】

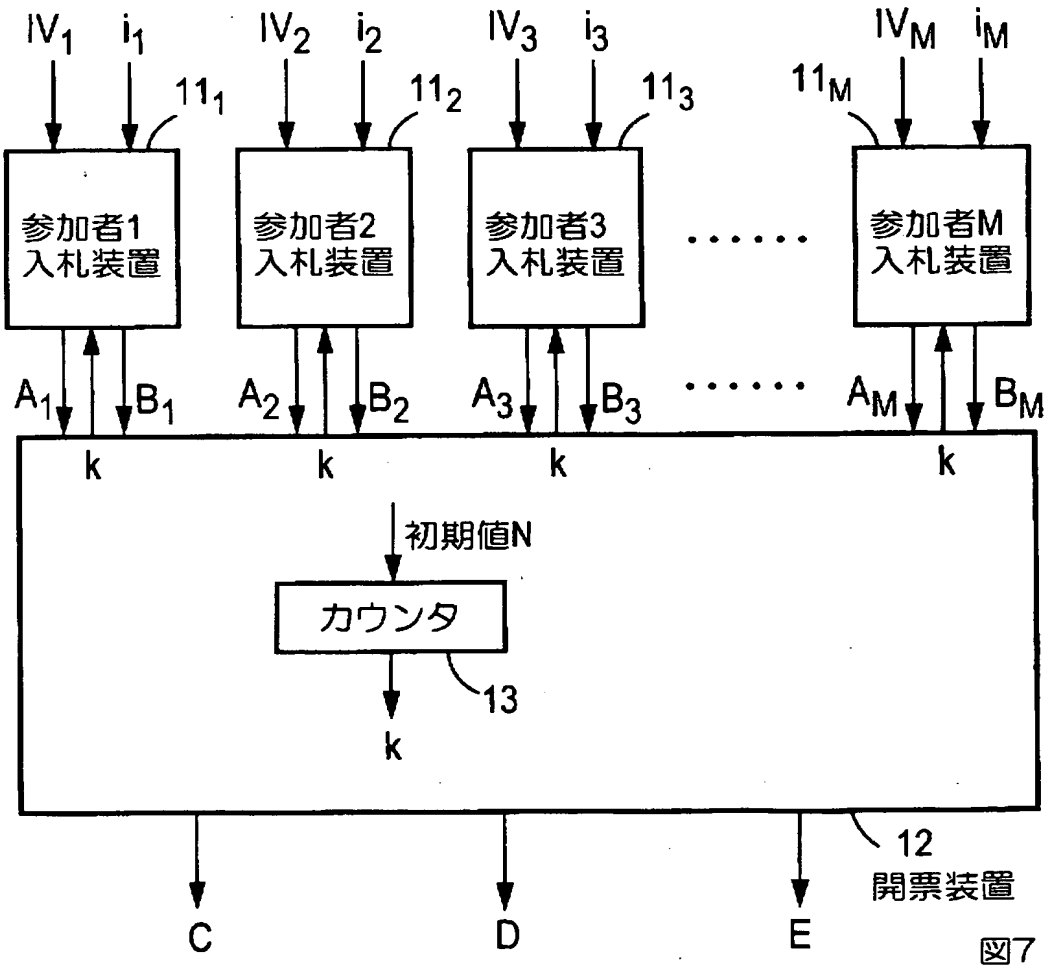

図7

【書類名】　　要約書

【要約】

【課題】　検証演算量を減少させる。

【解決手段】　各参加者ｊはＮ種の指標値１，２，…，Ｎから選んだ１つi_j、初期値IV_j、１以上の任意整数x_jを入力し、IV_jに対し一方向性関数をx_j回施して$g^{xj}(IV_j)$を求め、更に一方向性関数ｈをＮ－i_j回施して$A_j=h^{N-ij}(g^{xj}(IV_j))$を開票装置１２へ送って$i_j$を登録し、装置１２は全参加者からの$A_j$を受信後、ｋ＝Ｎ，Ｎ－１，…１と順次、ｋで登録したかを尋ね、参加者はｋと異なる値を登録した場合は$B_{k,j}=h^{k-ij-1}(g^{xj}(IV_j))$を、装置１２へ送り装置１２は$h(B_{k,j})=A_j$であることを確認して、$A_j$の値を$B_{k,j}$に変更し、ｋを登録した場合は参加者は$B_{k,j}=g^{xj-1}(IV_j)$を装置１２へ送り、装置１２は$g(B_{k,j})=A_j$を確認して、そのｋを登録した指標値の最大値とする。

【選択図】　　図１

出　願　人　履　歴　情　報

識別番号　　〔０００００４２２６〕

１．変更年月日　　１９９９年　７月１５日
［変更理由］　住所変更
住　所　　東京都千代田区大手町二丁目３番１号
氏　名　　日本電信電話株式会社